E-MAIL RETENTION POLICY

Policy Number: IOT 07-02

Issue Date: July 30, 2007
Effective Date: Immediate

1. Purpose

Establish guidelines and policy for preserving records creating using E-mail.

2. Revision History

Revision Date	Revision Number	Change Made	Reviser
07/01/07	01	Drafted Policies	C. Cotterill
7/25/07	02	Standard Formatting	C. Bradley

3. Persons, Groups, Systems Affected

IOT employees and individuals communicating with IOT via E-mail

4. Policy

All e-mail conducted on state government computers is owned by the State of Indiana and is a public record. Indiana Code 5-14-3-2(m) defines a public record as:

> [A]ny writing, paper, report, study, map, photograph, book, card, tape recording, or other material that is created, received, retained, maintained or filed by or with a public agency and which is generated on paper, paper substitutes, photographic media, chemically based media, magnetic or machine readable media, electronically stored data, or any other material, regardless of form or characteristics.

Anything, on any medium, that is created for any governmental purpose is subject to the terms of the public records law. Consequently, all e-mail messages sent or received for a government purpose are public records and are subject to record retention requirements ("Retention requirements" is a term used to refer to the rules set by the Indiana Oversight Committee on Public Records regarding the length of time different types of public records must be stored before they can be discarded.).

RECORDS CREATED WITH E-MAIL

Electronic mail systems can transmit a wide variety of information; therefore, the length of time that an e-mail has to be retained varies according to the content of the e-mail. In short, the content and *not* the medium determines how long an e-mail has to be retained.

E-mail messages fall within three broad categories:

1. Transitory & Duplicate messages or casual and routine communications - *No retention requirement*. Public officials and employees sending or receiving such communications may delete them immediately. Most e-mails are transitory. See section below for specific guidance on Transitory and Duplicate messages.

2. Public records with a less than permanent retention period - Follow retention period for equivalent hard copy records as specified in an approved retention schedule. See Appendix A for common IOT records that have a less than permanent retention period.

3. Public records with a permanent or permanent/archival retention period. See Appendix A for common IOT records that have a permanent retention period.

DEFINING TRANSITORY & DUPLICATE RECORDS

Transitory messages do not a) set policy, b) establish guidelines or procedures, c) certify a transaction, or d) become a receipt. Transitory documents serve to convey information of temporary importance. The following types of e-mail can be deleted because they are considered transitory:

- Incoming list serve messages
- Personal emails unrelated to state business
- Spam or unsolicited advertisements or sales promotions
- Non-policy announcements
- Telephone messages
- Published reference materials
- Invitations and responses to meetings, etc.
- Thank yous
- Replies to routine questions, "we're open 8 – 5", "our address is…", "the deadline is…"
- Scheduling meetings
- Out of Office auto-replies
- Attachments to e-mail that are identical to records that are stored and managed outside the e-mail system pursuant to approved record retention schedules

Internal Duplicate Records: E-mail as a medium promotes expedited communication to multiple users with great ease. Consequently, e-mail systems frequently contain duplicates of a record, such as copies or extracts of documents distributed for convenience or reference. "All Agency Memorandums" are often forwarded via e-mail within the State system in order to speed up distribution of certain critical and/or time-sensitive information. Information transmitted in this manner is simply a duplicate or non-record. If retention is required of the original, the *sender* has the obligation.

Accordingly, for an e-mail to qualify as a retainable "record" under this definition it must be documentation of the informational, communicative, or decision making process of state government that is;

1. Made or received in connection with the transaction of the public business or government functions; and

2. Which is created, received, retained, maintained or filed by the agency as evidence of its activities or because of the informational value of the data in the document.

Please see the ICPR General Retention and Disposition Schedule for Administrative Records for record retention requirements.[1] IOT's Record retention policy along with other agencies schedules can be found in the Retention Schedule Database.[2]

5. Responsibilities
   5.1. Indiana Office of Technology – All staff of IOT are responsible for reading, understanding and following the E-mail Retention Policy.

6. Procedures

I. Procedures for managing e-mail that must be retained

Each division of IOT must determine which record retention schedules apply to their commonly created and received records, including e-mail. Occasionally, areas may also need to review their retention schedules and request amendments and updates as necessary.[3]

Each employee is exclusively responsible for managing all the e-mail they send and receive; managing those e-mail means that each employee must sort, file, retrieve, and archive or delete the e-mail in accordance with these procedures.

a) **Sorting** involves promptly deleting e-mail when allowed by IC 5-15 and the applicable record retention schedule. Sorting also involves routinely filing e-mail that must be retained for the applicable retention period (see Appendix A for guidance on which record retention schedule may apply to a particular e-mail). To avoid wasting computer storage space, e-mail should be deleted promptly if it is not a record under IC 5-15 and if it has no further value.

b) **Filing** e-mail for short-term storage involves moving the e-mail into folders created within the e-mail software. For e-mails that must be retained for longer timeframes, it may also mean printing and filing hard copies of e-mail in a paper file or converting the e-mail into another software format for long-term electronic filing.

   When filing e-mail that qualifies for confidential treatment, it is a good idea to create a confidential folder and place it within the project folder so you have a place for the confidential e-mail that relate to that project.

   E-mail that qualifies as a retainable record under IC 5-15-5.1 must be retained in accordance the applicable record retention schedule that has been approved by the Indiana Commission on Public Records (ICPR). The content of the e-mail will determine which record retention schedule applies.

c) **Retrieving** e-mail means that, upon request, employees must promptly retrieve e-mail for which they are exclusively responsible (that is, sent or received from outside IOT). E-mail that is retrieved must include the transmission properties of the e-mail. Upon receipt of a public records request or discovery request, the IOT employee responsible for the requested

[1] http://www.in.gov/icpr/records_management/gr.html
[2] http://www.in.gov/icpr/records_management/rsintro.html.
[3] Record retention schedules can be created or updated in consultation with the Agency Record Coordinator and/or IOT's General Counsel and IOT's Records Coordinator. New or amended record retention schedules must be approved by the OCPR before becoming effective.

e-mail must find and retrieve it in a timely manner just as he or she must be able to quickly retrieve and produce paper documents in his or her possession or control. Each area of IOT will develop its own specific system for uniform file-folder creation and filing. This system should be based on, or consistent with, the area's paper filing system. Each area should also develop a system for how and when to convert e-mail to paper or microfiche for long-term storage. This long-term storage may be required based on applicable record retention schedules. These area-specific procedures will allow staff to more easily locate and retrieve e-mail.

d) **Archiving or deleting** filed e-mail must be done according to a record retention schedule approved by the ICPR. Archiving for the purposes of IC 5-15-5.1 involves the long-term storage of a record, including e-mail, according to the applicable retention schedule. ICPR requires all long-term archiving of records to be done in paper, microfilm or microfiche format. Currently, records can not be archived on electronic media. As always, the transmission properties of the e-mail are considered part of the e-mail and must be archived with the e-mail.

(1) The content of the e-mail determines the applicable retention schedule. Record retention schedules are maintained by each agency for agency specific records and approved through the ICPR process as well as the General Retention Schedule which applies to all agencies *(See Appendix A for guidance on how to ascertain which record retention schedule applies to an e-mail.)*.

(2) To avoid wasting computer storage space, e-mail should be deleted or archived promptly when authorized by the applicable retention schedule. However, records relevant to pending or reasonably anticipated litigation must be preserved even if a record retention schedule allows for its destruction. Such records will be subject to a litigation hold by the General Counsel.[4]

II. Procedures for managing e-mail when employees leave

a) Each employee is responsible for organizing, filing and archiving e-mail before leaving his or her position at IOT.

b) Supervisors are responsible for ensuring that their staff completes the final organization of e-mail before leaving. Supervisors are also responsible for managing, filing, retrieving and archiving the e-mail of their former staff.

III. Exceptions to Public Records Requirement and Confidential E-mails

Every e-mail written or received during the course of your work as a public employee is considered a "public record" by Indiana's Access to Public Records Act. This means the public has a right to inspect and copy every e-mail that a public employee writes or receives as part of his or her job unless the e-mail fits a specific exception to public disclosure. The IOT General Counsel responds to all public records requests.

a) **Exceptions to public disclosure requirements**

[4] Even if a record retention schedule provides for the destruction or alteration of a record (including an e-mail), if that record is relevant to "pending or reasonably anticipated litigation" it must be preserved as potential evidence in that litigation. Such records will be subject to a "litigation hold" by IOT's General Counsel or the Attorney General's office. If you believe a record is relevant to pending or anticipated litigation, check with IOT's legal counsel before destroying the record.

The Public Records Act specifically lists thirty-three types of records that may be kept confidential by a public agency.

b) **Confidential e-mail**

Every effort should be made to protect confidential information from disclosure and from losing its confidential status. Questions about an e-mail and its "confidential status" should be directed to IOT's General Counsel. (Your personal e-mails are not confidential.) E-mail that is intentionally or accidentally forwarded to someone outside IOT can lose its privilege. To ensure confidential information is properly protected, employees should do the following before including confidential information in an e-mail:

- Clearly label the e-mail as confidential, and warn the recipient not to forward the e-mail to anyone who is not authorized to receive it. Labeling the subject line of the e-mail as confidential in **bold face type** will make the confidentiality claim apparent when the e-mail is still in the recipient's inbox. This, in turn, will make it less likely that the recipient will accidentally forward the confidential e-mail to someone who is not authorized to see it.
- Create a signature block that claims the e-mail as confidential.
- Name the exception(s) to disclosure you are relying upon for the claim of confidentiality, including the statutory citation.
- Be aware that public employees who intentionally or knowingly disclose information that is classified as confidential commits a class A misdemeanor. In addition, an employee who recklessly discloses or fails to protect confidential information may be disciplined under personnel policies. See IC 5-14-3-10.
- Be aware that e-mail may be inadvertently transmitted to parties outside IOT, which can waive any claim of privilege.
- Be aware when sending extremely sensitive information, such as a company's trade secret, that it is possible for e-mail transmitted over the Internet to be intercepted and copied.
- Confirm whether a more secure form of communication is available or appropriate.

Permissible use of state resources

40 IAC 2-1-9 says: "A state officer or employee shall not make use of state materials, funds, property, personnel, facilities, or equipment for any purpose other than for official state business unless the use is expressly permitted by general written agency, departmental, or institutional policy or regulation, considering the cost and the benefit by such use."

IOT has adopted a *de minimis* use policy to guide employees and complies with the Information Resources Use Agreement.

7. Appendices

Appendix A

Examples of Common IOT Documents with Less than Permanent Retention Required

- REQUEST FOR CHANGE (RFC) SUPPORTING DOCUMENTATION .....1 year
  Test plans, test results, back-out procedures and other miscellaneous documentation used in the change process.

- INCIDENT RESPONSE .....5 years
  Notification of incident involving state information technology equipment or electronic data.

- PROJECT DOCUMENTATION .....10 years
  Documentation of agreement between IOT and another agency to provide services and/or equipment as well as bill for those services. Records may include project charters, statements of work (SOW), memoranda of understanding (MOU), project work plans, status reports and changes requested under the IOT project management process.

Examples of Common IOT Documents with Permanent Retention Required

- DISASTER RECOVERY AND CONTINUITY PLANS

Disaster Recovery/Continuity Plans for IOT, including those for electronic systems, as well as supporting documentation used in the development of the plans.